U.S. Department of Transportation
United States Coast Guard

Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol: G-CIM
Phone: (202) 267-1016

COMDTINST 5200.1
JAN 24 2002

COMMANDANT INSTRUCTION 5200.1

Subj: INFORMATION MANAGEMENT AND ELECTRONIC GOVERNMENT (E-GOV)

Ref: (a) Coast Guard Paperwork Management Manual, COMDTINST M5212.12 (series)
(b) The Coast Guard Freedom of Information Act and Privacy Acts Manual, COMDTINST M2560 M5260.3 (series)
(c) Policy on Coast Guard Use of Internet/Worldwide Web, COMDTINST 5230.56(series)

1. PURPOSE. Heightened use of the Inter/Intranets to conduct agency business, otherwise known as Electronic Government (E-GOV), is bringing about transformational change. The purpose of this Instruction is to ensure Coast Guard staff are aware of their legal and procedural responsibilities regarding content, format, maintenance and disposition of electronic records (e-records). Further, to promote E-GOV initiatives, this Instruction solicits submission of summaries of such projects/processes, which will be posted for agency-wide viewing.

2. ACTION. Area and district commanders, commanders of maintenance and logistics commands, commanding officers of headquarters units, assistant commandants for directorates, Chief Counsel, and special staff offices at Headquarters shall ensure compliance with the provisions of this Instruction.

3. DIRECTIVES AFFECTED. None.

4. DISCUSSION. We have moved beyond the first phase of merely having a presence on the Internet and are now striving to provide interactive Web service, which includes robust search capabilities and the ability to conduct transactions electronically. Citizen centric government will increasingly use the Internet to bring about transformational change. Agencies will conduct business with the public along secure Web-enabled systems, using portals to link common applications while protecting privacy. In addition to the public's enthusiasm for a Web-enabled government, recent legislation is strengthening our ability to convert to E-business processes while ensuring legal sufficiency. The Government Paperwork Elimination Act (GPEA)(http://cio.gov/Documents/implementation_gpea.html) requires that

DISTRIBUTION – SDL No.139

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	1	1	1		1	1	1	1	1	1		1	1	1	1	1	1	1	1		1		1	1	1	1
B	1	8	10	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
C	1	1	1	1	1	1	1	1	1		2	1	1	2	1		1	1	1	1	1	1	1	1	1	1
D	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1			1
E	1	1	1	1				1		1	1	1	1	1	1		1		1	1			1	1	1	1
F																	1	1	1							
G	1	1	1	1	1																					
H																										

NON-STANDARD DISTRIBUTION:

Federal agencies provide the option of submitting or disclosing E-information NLT October 2003. We are working on a number of initiatives throughout the Coast Guard. Initiatives include:

a. An electronic forms package that will provide users the capability of completing interactive e-forms via the Web.

b. The "Do-It-Yourself" (DIY) site on the Web allows citizens to pay for information requested under the Freedom of Information Act (FOIA) on-line.

c. The Certificates of Financial Responsibility System (COFRS). The National Pollution Funds Center (NPFC) is partnering with The Department of Treasury's Pay.Gov project to develop an e-commerce site for subject Certificates. Customers will be able to submit an application and user fees on-line.

d. Web Based Financial Document Imaging. The Coast Guard Finance Center (FINCEN) is partnering with the Department of Transportation (DOT) to provide a document imaging system that will integrate scanned images of commercial invoices with financial records in an automated system, thus making document images easily and quickly accessible over the Web.

e. The Human Resource Management Directorate has implemented software that will provide employees self-service capabilities for a number of transactions, as well as Web based employee survey systems. Information Technology training is also available on the Internet.

Further, GPEA strengthens the legal admissibility of E-signatures in court, paving the way for recognition of such signatures when needed. Commandant (G-CIT) is overseeing an effort to implement a Public Key Infrastructure (PKI) at Coast Guard such that appropriate levels of security can be applied to electronic transactions.

5. E-GOV INITIATIVES. To promote E-GOV initiatives, we are compiling a list of project summaries to post on Commandant (G-CIT's) Web site. Commands/units shall submit an abstract of their E-GOV projects/processes to http://cgweb.comdt.uscg.mil/g-si/e-gov/e-gov.htm.

6. DEFINITIONS. Following are terms discussed in this Instruction.

   a. Cookies. A cookie is a small piece of information sent to one's computer browser, along with a Web page, when a Web site is accessed. There are two types:

      (1) Session Cookies describe place keepers' technology used to retain content during an individual user session. They are discarded upon completion of a session or expire based on a short time frame and are not used to track personal information.

      (2) Persistent Cookies refers to a technology that collects user-identifying information such as extensive lists of previously visited sites, E-mail addresses, or other information identifying or building profiles on individual visitors to publicly accessible sites.

b. Electronic Government (E-GOV) is a broad term used to describe use of technology to enhance customer access to Government information and interactive services via the Web.

c. Electronic Signature (E-Signature) refers to the act of attaching a signature by electronic means. There are presently numerous forms of electronic signatures, ranging from biometric devices to digital signatures. The electronic signature process involves: authentication of the signer's identity; a signature process according to system design and software instructions; binding of the signature to the document; and non-alterability after the signature has been affixed to the document.

d. Information Life Cycle means the stages through which information passes: creation or collection, processing, dissemination, use, storage, and disposition.

e. Information System means a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.

f. Portal is a customized Web site serving as a gateway to enable users to expeditiously find agency information and answers to questions. Such a site categorizes information by topic and provides links to information and on-line services.

g. Public Key Infrastructure (PKI) is an established methodology for protecting information, ensuring data integrity, and authenticating systems users' identities. The enabling technology that makes ubiquitous electronic services over the Web secure is public key cryptography, which in combination with a PKI, ensures information security by also protecting confidentiality, providing digital signature capability, and supporting non-repudiation. A PKI involves a system of public keys, private keys, and certificates.

h. Records include all books, papers, maps, photographs, machine-readable materials or other documentary materials, regardless of physical form or characteristics, created or received by an agency of the U.S. government under Federal law or in connection with the transaction of public business. Records are preserved by an agency as evidence of the organization, functions, policies, decisions, procedures, operations or other activities, and for its information value. Electronic Records include any information as described above in a format requiring a computer or other machine for processing. They are preserved for the same length of time as scheduled paper records described in reference (a).

7. RESPONSIBILITIES. As we move forward with developing more electronic systems and conducting business electronically, several issues must be addressed to ensure secure transactions, protect proprietary information, and make information accessible to persons with disabilities.

a. Privacy. Clear privacy policies must be posted at principal Internet sites, major entry points to Web sites, and Web sites where Coast Guard or contractors acting on our behalf collect substantial personal information from the public. Note: On the Intranet (internal network), although access restrictions apply and personal data is protected, users should be aware that they are subject to

security monitoring, thus they should not have an expectation of privacy. Coast Guard Web sites, including those maintained by contractors on behalf of Coast Guard, shall comply with standards set forth in the Children's Online Privacy Protection Act of 1998 (http://www.ftc.gov/privacy/) with respect to collecting personal information online at Web sites directed to children. All Coast Guard staff, in particular Webmasters and Primary Content Approval Authorities (PCAOs), shall comply with the following with regard to the Internet:

(1) "Persistent cookies" are only authorized under the following circumstances:

(a) There is a compelling need to collect such information.

(b) Appropriate publicized technical procedures are established to safeguard the information.

(c) The collection has been personally approved by the Secretary of Transportation.

(2) "Session cookies" are authorized only if users are advised of what information is collected or stored, why it is being done, and how it is to be used.

(3) Web sites shall be periodically "scrubbed" for privacy and other sensitive information as defined in reference (b).

b. Releasability. The Internet Configuration Control Board (ICCB) has further established clear policy regarding content and format of information posted on the Web (reference (c)). It is incumbent on Coast Guard commands/directorates to ensure that information posted/released, including personal identifiers, falls within the scope of releasable data per the provisions of reference (b). See http://www.usdoj.gov/foia for more information on the Freedom of Information Act (FOIA) Program.

c. Information Assurance. Information Systems Security requires our attention such that potential harm is mitigated through cost effective controls to ensure that as we become more of an E-GOV organization our information is protected for confidentiality, integrity, authentication, availability, and non-repudiation. Citizen trust in on-line services is essential. Not only must personal information be secure, but also on-line information backed up by systems that are reliable. More information on electronic signatures and data encryption standards is available at http://csrc.nist.gov/cryptval/.

d. Electronic Records (E-Records). As programs consider eliminating the paper "source" document, the management of electronic records imposes additional requirements to ensure that data/documents are available throughout their Information life cycle. When converting a paper-based system to an E-system, program managers must ensure the following actions are taken: the National Archives and Records Administration (NARA) www.nara.gov must approve the conversion of a paper-based system to an electronic system. The legally required retention periods for electronic records are the same as those for paper outlined in reference (a). Further, long term funding must be allocated to upgrade/migrate the E-data/documents to ensure data integrity and readability. Other issues to consider are the stability of the E-media and the location of E-storage (i.e. on the hard drive or off-

loading onto disks, tapes, etc). Legal considerations for electronic records are discussed at http://www.cybercrime.gov/eprocess.htm.

e. Section 508 of the Rehabilitation Act sets forth a number of requirements for ensuring accessibility to information on the Web for persons with disabilities. More information is available at http://cgweb.comdt.uscg.mil/508/Section508/CG-Sec508Home.html.

V.S. CREA
Director of Information and Technology